NPS-CS-04-005

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

An Introduction to Legal Aspects of Operations in Cyberspace

by

Thomas C. Wingfield and James B. Michael

28 April 2004

Approved for public release; distribution is unlimited.

Prepared for: Naval Postgraduate School Homeland Security Leadership Development Program, under the auspices of the U.S. Department of Justice

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

RDML Patrick W. Dunne
Superintendent

Richard S. Elster
Provost

This report was prepared for the Naval Postgraduate School Homeland Security Leadership Development Program's curriculum for the Homeland Defense specialization of the Master of Arts degree in National Security Affairs and funded by the U.S. Department of Justice.

This report was prepared by:

_____
James Bret Michael, Associate Professor
Department of Computer Science

Reviewed by:

_____
Peter J. Denning, Chairman and Professor
Department of Computer Science

Released by:

_____
Leonard A. Ferrari
Associate Provost and Dean of Research

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** 4/28/04	**3. REPORT TYPE AND DATES COVERED** Technical Report	
4. TITLE AND SUBTITLE: An Introduction to Legal Aspects of Operations in Cyberspace			**5. FUNDING NUMBERS** 2002GTR057
6. AUTHOR(S) Thomas C. Wingfield and James B. Michael			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER** NPS-CS-04-005
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Department of Justice Washington, DC			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this technical report are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

This report consists of a learning module on the legal aspects of operations in cyberspace. The learning module was developed specifically for use in the Naval Postgraduate School Homeland Security Leadership Development Program's curriculum for the Homeland Defense specialization of the Master of Arts degree in National Security Affairs. Given the complexity of the law governing cyber operations, it is vitally important that policymakers and their legal advisers share a common intellectual framework for evaluating and responding to attacks in cyberspace. This learning module provides the student with an introduction three overlapping legal regimes within which to conduct cyber operations: law enforcement, intelligence collection, and military operations.

14. SUBJECT TERMS **15.** Law, Cyberspace, Homeland Security, Homeland Defense, Law Enforcement, Intelligence Collection, Military Operations	**15. NUMBER OF PAGES** 20
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UL

Standard Form 298 (Rev.2-89)

THIS PAGE IS INTENTIONALLY LEFT BLANK

An Introduction to Legal Aspects of Operations in Cyberspace

Learning Objectives

At the completion of this learning module, the student will be able to do the following:

- Identify the three legal regimes governing operations in cyberspace
- Describe the fundamental aspects of the law enforcement paradigm, including its primary strengths and weaknesses in dealing with cyber intrusions
- List the types of computer crimes
- Explain the general bases for limiting search and seizure by government, including the requirement for a search warrant the exceptions to this rule
- Explain the concept of "reasonable expectation of privacy"
- Describe limits on workplace searches, distinguishing them from other searches
- Explain the general bases for government surveillance
- List the requirements of, and the exceptions to, the Wiretap Act and the Electronic Communications Privacy Act
- Describe the nature of entrapment
- Describe the fundamental aspects of the intelligence collection paradigm, including its primary strengths and weaknesses
- List the requirements for "U.S. Person" status
- Describe the fundamental aspects of the military operations paradigm, including its primary strengths and weaknesses
- Identify the two primary legal questions in the military operations paradigm
- Explain the origin of the Schmitt Analysis, its seven criteria, and the process by which it resolves *jus ad bellum* questions
- List and define the four customary principles of the law of armed, explaining how each applies to operations in cyberspace
- Describe the applicability of air law, space law, and the law of the sea to cyber intrusions
- Distinguish homeland defense from homeland security
- Briefly explain the basis for the doctrine of *posse commitatus*
- Describe the role of decoys in cyber operations

Executive Summary

There are three legal paradigms through which to characterize computer intrusion. These paradigms overlap each other. In addition, an intrusion can fit into any two or all three of the paradigms. They are:

- Law Enforcement
    - almost all computer intrusions can be dealt with under this paradigm
    - there are two levels of domestic legal authorities: federal and state statutes
    - there is an evolving body of international criminal law
    - LE can be applied to most threats, but is not effective against all threats
    - LE also involves strict evidence-collection rules which limit potential defensive responses
    - In addition to government criminal sanction (prison time/fines; beyond a reasonable doubt), numerous civil remedies (damages; preponderance of evidence(lower standard)) exist for government and private individuals

- Intelligence collection
    - intelligence operations may only be conducted against non-U.S. persons
    - after this categorical determination, almost nothing can be collected on U.S. persons and almost anything can be collected on non-U.S. persons
    - a U.S. person is a U.S. citizen, a resident alien, a U.S. corporation, or an organization composed substantially of Americans.

- Military operations
    - only those intrusions that may be characterized, either independently or in conjunction with other such actions, as a use of force under international law or are part of an ongoing conflict may be dealt with militarily
    - posse comitatus is complex legal doctrine but it does permit domestic military operations (homeland defense v. homeland security)
    - two primary questions in this field:
        - Are we at war?
            - UN Charter paradigm
            - Schmitt Analysis
        - If we are at war, what rules apply?
            - Discrimination
            - Necessity
            - Proportionality
            - Chivalry

The legal challenge in any computer intrusion is properly characterizing the intruders' categorical legal identity. This will determine whether one or more of the above paradigms are applicable. Each as has strengths, weaknesses, and limitations. Each also requires that an intrusion be dealt with according to its own precise standards.

LAW ENFORCEMENT

Law Enforcement is the most ubiquitous of the three legal approaches to intrusions in cyberspace. It is based in the domestic law of the country which suffers the

intrusion, and is intended to deal with intruders as individuals or, at most, small conspiracies of a few people. The law enforcement paradigm in the United States is one of patient, painstaking evidence collection under tight constitutional and statutory limitations. Presumptions favor the accused, and investigations are undertaken with an eye toward prosecution and incarceration. It may operate against U.S. citizens, non-citizens within U.S. control, or citizens of other countries having extradition agreements with the U.S. Such agreements are possible only when each state party has a domestic law criminalizing the same behavior.

The strengths of this approach are the clarity of its rules and (relative) certainty of its processes. It provides a highly transparent means by which to identify and sanction bad actors in cyberspace, and allows for highly individualized treatment in different cases. The weaknesses include the slow pace of investigation (especially at the federal level), the need to apprehend the accused, and the advantage to which an intruder may put the numerous limitations on government action against him.

Computer Crimes[1]

Computer crimes fall into two broad categories: those with a target in cyberspace, and those which merely employ computers as a means toward a more traditional criminal end. The first type includes attacks on the confidentiality, integrity, or availability of information or systems. These crimes also include the theft of computer-stored information or cyber-based services. Computer intrusions of this type include:

- Damaging computer systems
- Trespassing
- Threatening damage
- Impairing the integrity and confidentiality of a network

Theft of information usually involves one of three categories: government (military of law enforcement), business information (trade secrets or confidential information, such as business plans), and financial information (account numbers and electronic fund transfers). Theft of services may include "phreaking" (penetration of a telephone switching system to steal long-distance calling services), stealing passwords, or establishing shell accounts. The second type, in which the computer is an instrumentality of the crime, includes gambling, child pornography, espionage, stock fraud, bank fraud, and copyright piracy.

Search and Seizure

The law dealing with government search and seizure begins with the Fourth Amendment to the U.S. Constitution:

[1] This section is based upon the work of Clement McGovern of the U.S. Department of Justice Computer Crime and Intellectual Property Section, included in his presentation *Searching and Seizing Computers and Electronic Evidence.*

> The right of the people to be secure in their persons against unreasonable searches and seizures shall not be infringed, and no Warrants shall issue without probable cause, supported by Oath or affirmation, and particularly describing the place to be searched an the persons or things to be seized.

Government searches, then, may be undertaken when:

- A warrant has issued,
- Government conduct does not violate the a person's reasonable expectation of privacy, or
- A specific exception to the warrant requirement applies.

Reasonable Expectation of Privacy

Reasonable expectation of privacy (REP) contains subjective and objective prongs. A person has a REP when his conduct reflects an actual subjective expectation of privacy, and that expectation is objectively reasonable under society's expectations. In U.S. v. Katz and subsequent cases, the U.S. Supreme Court found REP in homes, phone booths, and opaque containers, but not in garbage, public activities, or a stranger's home. These examples have provided the basis for analogies in cyberspace, particularly the search of e-mail. Messages may be stored on the sender's system, on the recipient's e-mail server, or on the recipient's own machine. REP may be lost id one relinquishes control of one of these systems to a third party, such as a repair shop or a friend. Fourth Amendment protections apply only vis-à-vis the federal government (or, though the Fourteenth Amendment, state and local governments) and do not restrict private searches, so long as the private party is not acting as an agent of the government. The presence of REP in opaque containers extends to the information stored in computer systems, including hard drives, personal digital assistants, and pagers.

Exceptions to the warrant requirement include:

- Consent
- Exigent circumstances
- Plain view
- Search incident to lawful arrest (SITA)
- Inventory search
- Border search
- Private party search

When an individual grants consent, the scope of that consent is a key question. The test, established in the Supreme Court case *Florida v. Jimeno,* is what a reasonable person listening to the granting of consent would think. This test is highly fact-specific and varies from situation to situation. To avoid future questions regarding the scope of consent. Law enforcement officers are encouraged to obtain the consent in written form, expressly specifying the systems to be accessed.

Third parties may, under certain circumstances, grant consent for a search. Under *U.S. v. Matlock* and subsequent cases, a private person who shares common authority or control over a computer may grant consent. This usually includes the target's spouse, may include the target's roommate or co-workers, and usually does not include computer repairmen or government officials. Password protection or encryption may defeat third party consent.

The results of private searches may be shared with government officials after the fact, assuming no prior agency relationship. Under *U.S. v. Jacobsen*, law enforcement officers may see what the private person saw, but no more. This approach is very common in computer cases.

Under *U.S. v. Horton*, items in plain view may be seized if their incriminating nature is immediately apparent. *U.S. v. Hall* permits a computer to be seized (but not accessed) temporarily until a warrant issues, but *U.S. v. Carey* forbids searches based on nothing more than an opinion that the contents of a system are incriminating based merely on the filename and type.

In *U.S. v. David* the Supreme Court held that exigent circumstances permit the seizure and search of a computer system to prevent the destruction of evidence. This exception is often applied to the volatile information stored in the pagers of criminal suspects. This exception, however, lasts only as long as the exigency, and once the evidence is safely out of danger, a warrant is required for any subsequent search.

A search incident to arrest (SITA) permits reasonable searches of a person and the electronic devices on his person (*e.g.*, pagers, cell phones, and PDAs) at the time of arrest.

An inventory search is permitted following arrest for the non-investigatory purpose of establishing an accurate record of the suspect's property. Theses searches may yield evidence, but only if originally undertaken for the purpose of inventory. In *U.S. v. Flores*, a case in the Southern District of New York, the court held that there was no legitimate non-investigatory purpose in searching the contents of a suspect's cell phone—that a lawful inventory search would require no more than recording the presence of the cell phone, and not its contents.

Warrantless searches are permitted at the U.S. border. In *U.S. v. Roberts*, federal authorities set up a false inspection station at an airport in order to catch a suspect before his flight to Paris. The court held that the thousands of child pornography images seized were within the scope of the exception and admissible against the defendant.

Workplace Searches

In the workplace, employees retain REP unless the objects or information are open to the world at large. An employer may consent to the search of an employee's

workspace. In *O'Connor v. Ortega*, the Supreme Court established a unique test for public employment workplace searches. If the workplace to be searched is "open to fellow employees or the public," *or* if there are "actual office practices and procedures . . . or legitimate regulations" that permit a search, then there is no REP.

The Fourth Circuit, in *U.S. v. Simons*, has held that a properly worded banner is sufficient to destroy REP. One example of such a banner is: "This is a government computer network. You should have no expectation of privacy in your use of this computer. Your use constitutes consent to monitoring."

A written employment policy may serve the same purpose. In the absence of such a banner or policy, a public employment search may still be permissible (under *O'Connor*) if reasonable in scope and duration. The search must be justified at its inception, reasonably related in scope and circumstances, and be conducted by employers for work-related purposes (*i.e.*, retrieving a file or conducting a workplace misconduct investigation).

Government Surveillance[2]

The Wiretap Act (18 U.S.C. §§2251-2522) forbids government interception of wire-based communications unless a specific exception applies. Exceptions include:

- Court Order
  - Probable cause that communication facility being used in crime, interception will reveal evidence of the predicate felony
  - Normal investigative techniques (subpoena, pen register, trap and trace, undercover agents, search warrants, surveillance, interviews and informants) have been tried and have failed, or would be unlikely to succeed
- Consent
  - Granted by a party to the communication
  - Bannering, terms of service, or employment policies may provide constructive consent
- Provider Protection
  - Monitoring must be done to protect the ISP's rights or property (including intangible property)
  - Provider may give results of *past* monitoring to law enforcement; may not be tasked by law enforcement
  - Extent of this exception is not well defined
- Computer Trespasser
  - Target has no contractual relationship with the government or authority to be on the computer, and

[2] The material in this section is drawn from the work of Richard Salgado of the U.S. Department of Justice, and is contained in his 2003 presentation.

    - ISP has authorized interception, and
    - Government does the monitoring, and
    - The interception is relevant to an ongoing investigation
- Extension Telephone
- Inadvertently Obtained
- Accessible to Public

The Electronic Communications Privacy Act (ECPA) controls government access to stored communications and transactional records. It provides criteria for voluntarily providing evidence to the federal government and a specific process to compel (nonvoluntary) production. Voluntary disclosure by the ISP is permitted only when the service in question is offered "to the public." Precisely how much of the public to whom the service must be offered is still unsettled.

Under ECPA, content receives more protection than non-content, and voicemail is treated identically to e-mail. There are three types of process for obtaining this information:

- Subpoena: basic subscriber information
- Court order: 2703(d) orders for above and transaction logs
- Search warrant: above plus content (unopened e-mails)

As general rules, more process yields more information, and more process reduces the requirement to give advance notice to the subject.

A 2703(d) order requires " . . . specific and articulable facts showing that there are reasonable grounds to believe that [the requested records] are relevant and material to an ongoing criminal investigation." The order may include a directive to the provider not to disclose to subscriber. The orders are effective nationwide, and may be issued by federal or state courts. 2703(d) orders may also be used in place of a subpoena to obtain communications not in electronic storage from a public provider, but prior notice must be given. This notice mat be delayed, and may include a directive to provider not to disclose to subscriber.

2703(f) request requires provider to preserve record for 90 days to allow law enforcement to seek proper authorization for search and seizure. This duty extends only records in the provider's possession at the time of the request, not future information. These requests may be extended.

2702 governs voluntary disclosure prohibitions and exceptions. A private provider may disclose all contents, whether retrieved or not, transactional data, and user information. A public provider must follow the more narrow statutory exceptions:

- Consent to disclose exists (*e.g.*, banner)
- To protect rights and property

- If contents are inadvertently obtained and pertain to the commission of a crime, or
- If the provider reasonably believes an emergency involving immediate danger of death or serious bodily injury requires disclosure

Violations of ECPA are remedied by civil damages only. There is no suppression remedy for a non-constitutional violation.

ECPA recognizes three broad types of evidence—basic subscriber information, transactional records, and content—and is structured around a series of dichotomies:

- Content of communications v. non-content
  - Content: retrieved e-mail v. non-retrieved
    - Retrieved e-mail: held by public v. private provider
      - Public provider: protected by ECPA requires notice to compel disclosure
      - Private provider: normal subpoena; no notice required
    - Unretrieved e-mail: stale (>180 days) v. fresh (<180 days)
      - Fresh, unretrieved content: requires search warrant
        - No notice to intended recipient is required
  - Non-content: detailed transactional v. basic subscriber information
    - Basic subscriber information
      - Obtained through subpoena
      - Includes:
        - name and address
        - local and long distance telephone billing records
        - telephone number or username or screen name
        - length and type of service provided
        - session times and duration
        - temporarily assigned network address
        - means and source of payment
    - Other non-content
      - Includes:
        - Audit trails and logs
        - Identities of e-mail correspondents
        - Cell site data
      - Obtained through 2703(d) court order

Entrapment

Entrapment is not the product of a specific stature, but is a legal defense in criminal prosecutions. It does not apply in civil cases. Entrapment has two requirements: The government must induce the illegal conduct, and the defendant must not have been

predisposed to engage in the illegal conduct. This two-part test is a difficult one for the defendant to prove, and is thus rarely successful. There are also numerous bases for civil liability in deploying honeypots. Any reasonably foreseeable damage caused to an innocent party may provide grounds for a suit for monetary damages.

For further information, the best single website on the criminal aspects of cyber intrusions is http://www.cybercrime.gov/.

INTELLIGENCE COLLECTION

Intelligence Collection is the simplest of the three legal approaches to cyber operations. There is only one major test: Is the target a U.S. person? If the intruder is a U.S. citizen, a resident alien, a group with a substantial number of American members, or a U.S corporation, then the U.S. intelligence community has virtually no power to collect against him. If, however, the target is a foreign national not falling into a protected category, there are remarkably few limitations on collection. The laws and directives governing the intelligence community are scrupulously followed, in large part because of the aggressive oversight maintained by the cleared members and staff of the House and Senate intelligence committees.

This paradigm offers great freedom for prompt and intrusive collection against those not protected by the U.S. Constitution. The primary aim under this approach, however, is not immediate resolution, but maximum information collection. An intruder may be left to his own devices indefinitely, in the hopes of learning as much as possible about him. Questions would include: What information is he seeking? What techniques is he using? Who is working with him? What organization or government is supporting him? Once the purely intelligence-gathering portion of the operation is mature, it may even be possible to launch a counter-intelligence operation, feeding him false information to act as a tracer, or to alter the adversary's decision-making. The weakness here, then, is that an intruder may "get away with it" for quite some time, and the Big Picture of the intelligence community may rationally demand that a few systems be compromised to provide the information needed to protect the greater good.

MILITARY OPERATIONS

The law governing the resort to and execution of military operations is the third major area of the law governing activities in cyberspace. This last category has three distinct regimes, depending on the phase of any given conflict: the law of peace (*jus in pace*), the law of conflict management (*jus ad bellum*), governing the transition from peace to war, and the law of war (*jus in bello*). Before evaluating the efficacy of any policy choice, decision-makers must have sound, fact-based legal advice that is

connected to clearly articulated principles of law. *See generally* Schmitt 1999 and Wingfield 2000.

Of central importance is the application of the law of armed conflict to the use of force by states in cyberspace once hostilities have commenced. At a point along the spectrum of interstate activities called the line of belligerency, a use of force by a state establishes an international armed conflict as a matter of law and the law of armed conflict applies. Even though the law of conflict management continues to apply during armed conflict, the law of armed conflict specifically authorizes a state to use all necessary and proportional force not otherwise prohibited by the law of armed conflict that is required for the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources.

The two principal questions facing military operators in cyberspace, then, are:

> (1) which interstate activities in cyberspace constitute a threat or use of force under international law, and
>
> (2) when such a threat or use of force does constitute an armed attack under international law, how does the law of armed conflict apply to the lawful exercise of the inherent right of self-defense in cyberspace?

These questions are fundamental to the law of information conflict (LOIC), which is the composite of the peacetime regime of international law, the law of conflict management, and the law of armed conflict that regulates the conduct of all state activities in cyberspace. It embodies the application of the entire peacetime regime as well as the entirety of the laws of conflict management and armed conflict to state activities in cyberspace.

The first of these questions has been problematic for quite some time. Until recently, the consensus among top legal scholars in the US and abroad was that a *quantitative* approach to cyber-warfare made the most sense. That is, when evaluating whether an information operation rose to the level of a use of force or armed attack, one should disregard the means and focus exclusively on the ends. Whether an oil refinery is set ablaze from a one-ton bomb or from a line of malicious computer code doesn't matter. A flaming refinery, they concluded, is a flaming refinery. Any cyber-attack that causes damage indistinguishable from a kinetic attack should be legally indistinguishable as well.

There is, unfortunately, a catch—the UN Charter, the paradigmatic document of international law, takes a *qualitative* approach, not a quantitative one. The framers, writing at the end of WWII, wanted to discourage military coercion, even at the cost of increasing diplomatic and economic coercion. Deciding that even the most stiffly worded diplomatic note—or restrictive economic boycott—would be preferable to an armored division crashing across an international border, the framers incorporated a very low threshold for impermissible military activity and a very high threshold for nonmilitary activity. The problem with this approach, as the subsequent decades have

shown, is that many forms of "nonmilitary" coercion—such as terrorism and so called "low intensity conflicts"—result in more death and destruction than many traditional military activities, and many of today's information weapons look nothing like military weapons and technology of the past. Sixty years ago, a telegraph message was simply a means of communication, benign and unassuming. Perhaps today—and certainly in the future—its e-mail equivalent could carry a virus capable of wreaking just the sort of havoc described above.

Policy makers can overcome this intellectual and legal quandary by adhering to a forward-looking doctrine known as the "Schmitt Analysis." By demonstrating *how* military coercion differs from diplomatic and economic coercion, Michael Schmitt, late of Yale, the Naval War College, and now at the Marshall Center in Europe, identified seven areas—severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility—in which military operations differ qualitatively from nonmilitary ones. If any given operation were quantitatively "graded" in each of these seven areas, the results could be used to give a principled qualitative description of the operation, accurately classifying it as a use of force or not. In short, the quantitative input suggested by the world's leading scholars on the topic would yield the qualitative output required for a proper characterization under the UN Charter.
This analysis has the added advantage of requiring attorneys and their clients to make conscious, documented assessments of each facet of a proposed operation, educating them in an otherwise subjective, opaque, and often incomplete *ad hoc* analysis. This is as true of planning an offensive operation as it is of analyzing, and reacting lawfully to, an attack in which we are the victims.

How specifically should decision-makers use this information to think more clearly about ordering such operations? Here are the dyads they should keep in mind:

- Severity: If people are killed or there is extensive property damage, the action is probably military; the less damage, the less likely the action is a "use of force."
- Immediacy: When the effects are seen within seconds to minutes—such as when a bomb explodes—the operation is probably military; if the effects take weeks or months to appear, it is more likely diplomatic or economic.
- Directness: If the action taken is the sole cause of the result, it is more likely to be viewed as a use of force; as the link between cause and effect attenuates, so does the military nature of the act.
- Invasiveness: A violated border is still an indicator of military operations; actions that are mounted from outside a target nation's borders are probably more diplomatic or economic.
- Measurability: If the effect can be quantified immediately—such as photographing a "smoking hole" where the target used to be—the operation has a strong military characteristic; the more subjective the process of evaluating the damage, the more diplomatic or economic.

- Presumptive Legitimacy: State actors have a monopoly on the legitimate use of kinetic force, while other non-kinetic actions—attacks through or in cyberspace— often are permissible in a wider set of circumstances; actions that have not been the sole province of nation-states are less likely to be viewed as military
- Responsibility: If a state takes visible responsibility for any destructive act, it is more likely to be categorized as a traditional military operation; ambiguous responsibility militates for a non-military label.

The Schmitt Analysis lends itself to partial automation, and several articles have been published on the topic. *See* Farkas, *et al.*, 2004.

Once the determination has been made that a state of *de facto* hostilities do exist and the law of armed conflict does apply, the analysis turns to the four central principles of the law of war: discrimination, necessity, proportionality, and chivalry.

The principle of *discrimination* requires that, prior to any use of force, the attacker distinguish between combatants and noncombatants, between military objectives and civilian objects. Noncombatants include civilians and "protected persons," such as medics and chaplains. While it is unlawful to attack civilian objects as such, it is not unlawful to collaterally damage civilian objects located so close to lawful military objectives that no reasonable precautions could have prevented the damage. In cyberspace, such distinctions will require the collection and analysis of information to produce the intelligence required to make such determinations. The military commander must consider foreseeable secondary effects in his target selection and mission planning.

The principle of *necessity* permits the use of all force required for mission accomplishment and force protection, but not superfluous force or unnecessary suffering. Superfluous force is that which is inflicted solely for the sake of causing damage. Unnecessary suffering has two components: quantitatively, it is simply the complement of military necessity (necessary force); qualitatively, it includes those means and methods of war that are by nature inhumane (chemical weapons, biological weapons, exploding bullets, transparent bullets which cannot be detected in the body by x-ray equipment).

The principle of *proportionality* requires the military commander to balance the collateral damage (against civilians and their property) of a planned attack against the concrete and direct military advantage expected to be gained. Proportionality is *not* the requirement to respond with only as much force as was used in the precipitating attack, and is *not* the requirement to employ the same means and methods as in the provoking attack. Whatever other policy preferences may be expressed later in the national security decision-making process, the basic legal requirement is to ensure the balance of military advantage gained outweighs the damage done to noncombatants and their property.

The principle of *chivalry* permits ruses of war, but forbids perfidy. Perfidy is unlawfully deceiving an opponent that he is entitled to enjoy, or required to accord, protections of law, which are, in fact, inapplicable in the situation. Attacking an enemy

facility from a vehicle displaying the Red Cross or the U.N. flag would be examples of perfidiously deceiving the enemy into according protections under law (not attacking the vehicle) which are not applicable. Broadcasting a false notice of cease-fire or calling for a *parlementaire* before attacking the unwary opponent would be an example of perfidiously deceiving one's opponent that he is entitled to a protection of law, which in fact, he is not. Ruses of war, on the other hand, are legal. They are wartime deceptions that convince an enemy to launch or withhold an attack based on tactical reasons, rather than perceived legal reasons.

Treaty law reflects the four basic principles of discrimination, necessity, proportionality, and chivalry, described above, codifying and implementing customary international law. They occasionally lead international law by affirmatively proposing new norms and standards, at first applicable to only those nations which sign the agreements. Such new standards may become binding on other nations over time, if those other nations adopt the new norms, and do so out of a sense of legal obligation. Treaties applicable to an earlier age or a different type of warfare may nonetheless be useful in charting the course of the law of information conflict, to the extent that analogies may be drawn from them and applied to operations in cyberspace.

In addition to treaty law, there is another legal dimension, based on the various geographical regimes implicated by a contemplated course of action. The principle areas are the law of the sea, air law, space law, and foreign domestic (or host nation) law. The law of the sea addresses the metaphor of "innocent passage" in cyberspace, unauthorized broadcasting, and liability for damage done in wartime. Air law covers the metaphor of defining airspace (as applied to defining cyberspace), the legal restrictions on interfering with aircraft communications or navigation, as well as physical attacks on aircraft. Space law is useful in the distinction of air and space, the use of space platform for peaceful and non-peaceful purposes, and the liability of those who cause damage against or through the use of space platforms. Foreign domestic law is most applicable in the area of stationing arrangements and the limitations they place on the employment of weapons and forces forward deployed.

Finally, in the international arena, there is the rapidly-developing law of Computer Network Espionage (CNE) and Computer Network Attack (CNA), which are located on two places along the spectrum of conflict, and have distinctly different legal characteristics. Computer Network Espionage, like any form of pure espionage, is lawful under international law, but is usually not lawful under the domestic law of the target state. CNE usually involves little or no force, and involves only as much intrusion as is necessary to collect the required information from the adversary's systems. Computer Network Attack, on the other hand, involves some kind of destruction with consequences in the physical world. CNA should be analyzed as any other type of use of force, and, depending on the scope, duration, and intensity of the force employed, may rise to the level of an armed attack.

While these questions are almost exclusively within the field of international law, the War on Terror has raised questions regarding the domestic aspects of military

operations—specifically, the proper delineation of *homeland security* from *homeland defense*. In general terms, *homeland defense* is the domestic use of military forces against foreign enemies, and *homeland security* includes most everything else. This distinction is captured in the long-enduring but poorly understood doctrine of *posse comitatus*. Under the current understanding of the doctrine, the military is forbidden to act domestically in a law enforcement capacity vis-à-vis U.S. citizens, but may perform traditional military missions against foreign enemies on U.S. soil. The scope and pedigree of this doctrine are complex and are often applied more as a matter of policy than law. A comprehensive treatment of this topic is beyond the scope of this learning module, but the definitive article on the topic, Felicetti and Luce (2003), is currently available.

Given the complexity of the law governing this new area of operations, it is vitally important that policymakers and their legal advisers share a common intellectual framework for evaluating and responding to attacks in cyberspace.

ADDITIONAL TOPICS

Decoys

Honey pots, honey nets, and decoys have received a great deal of attention in recent years as a means for diverting, containing, and studying cyber intrusions. Several articles stand out as excellent introductions to the legal, policy, and technical considerations in developing, testing, deploying, and operating cyber decoys. *See generally* Auguston, *et al.*, 2002; Michael 2002; Michael and Riehle 2001; Michael and Wingfield 2003; Michael, *et al.*, 2003A; and Michael, *et al.*, 2003B.

BIBLIOGRAPHY

M. Auguston, N. Rowe. J.B. Michael, and R.D. Riehle. Software Decoys: Intrusion Detection and Countermeasures. In *Proc. Workshop on Information Assurance,* pp. 130-39. IEEE, 2002.

C. Farkas, T.C. Wingfield, J.B. Michael, and D. Wijesekera. THEMIS: Treat Evaluation Metamodel for Information Systems. Publication pending, 2004.

G. Felicetti and J. Luce. The Posse Comitatus Act: Setting the Record Straight on 124 Years of Mischief and Misunderstanding before Any More Damage is Done. 175 Mil. L. Rev. 86 (March, 2003).

J.B. Michael. On the Response Policy of Software Decoys: Conducting Software-Based Deception in the Cyber Battlespace. In *Proc. of the 26th Annual International Computer Software and Applications Conference*, pp. 957-62. IEEE 2002.

J.B. Michael and R.D. Riehle. Intelligent Software Decoys. In Proc. *Monterey Workshop on Engin. Automation for Software-Intensive Syst. Integration,* pp. 178-87. Monterey, CA: ARO/ONR/NSF/DARPA, 2001.

J.B. Michael and T.C. Wingfield. Lawful Cyber Decoy Policy. In S.D.C. Vimercati, P. Samarati, D. Gritzalis, and S. Katsikas, eds. *Security and Privacy in the Age of Uncertainty*, pp. 483-88. Norwell, MA: Kluwer Academic Publishers, 2003.

J.B. Michael, G. Fragkos, and M. Auguston. An Experiment in Software Decoy Design: Intrusion Detection and Countermeasures via System Call Instrumentation. In S.D.C. Vimercati, P. Samarati, D. Gritzalis, and S. Katsikas, eds. *Security and Privacy in the Age of Uncertainty*, pp. 253-64. Norwell, MA: Kluwer Academic Publishers, 2003.

J.B. Michael, G. Fragkos, and D. Wijesekera. Measure Response to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System. In *Proc. 27th Annual International Computer Software and Applications Conference*, pp. 621-27. IEEE, 2003.

M.N. Schmitt. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Research Publications 1, Information Series, 1999.

T.C. Wingfield. *The Law of Information Conflict: National Security Law in Cyberspace.* Aegis Research Corp., 2000.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Ted Lewis
   Naval Postgraduate School
   Monterey, California

4. Professor J. Bret Michael
   Naval Postgraduate School
   Monterey, California